



## FEDERAL BUREAU OF INVESTIGATION POLICY DIRECTIVE

### Importing Nontransitory Records Into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats 1001D

#### General Information

<b>Proponent</b>	Records Management Division (RMD)
<b>Publication Date</b>	2018-01-08
<b>Review Date</b>	2021-01-08
<b>Last Updated</b>	N/A
<b>Supersession</b>	Policy Directive (PD) 0671D, <i>Importing Non-Transitory Records into Sentinel and Preserving Certain Investigative Non-Transitory Records in Original Format</i>

#### 1. Authorities

- Title 44 United States Code (U.S.C.) Chapters 21, 29, 31, and 33 (Federal Records Act)
- Title 36 Code of Federal Regulations (CFR) Chapter 12, Subchapter B, "Records Management"
- Federal Rules of Criminal Procedure Rule 16
- Federal Rules of Civil Procedure Rule 34

#### 2. Purpose

The purpose of this PD is to ensure that Federal Bureau of Investigation (FBI) personnel scan and import nontransitory, hard-copy records (needed for more than 180 days) into Sentinel, and maintain and preserve original hard copies of certain nontransitory investigative records (as further described in subsection 5.3. of this PD).

#### 3. Scope

This policy applies to all FBI personnel.

#### 4. Exemptions

- 4.1. Subsection 5.3. of this PD does not apply to security records for FBI personnel or applicants because those documents are administrative records, not investigative.
- 4.2. This policy does not apply to the handling of physical, digital, or electronic surveillance (ELSUR) evidence. For guidance on these matters, please see the *Field Evidence Management Policy Guide* (0780PG), *Digital Evidence Policy Guide* (0830PG),

**UNCLASSIFIED**

*Advanced Electronic Surveillance and Searches Policy Directive and Policy Guide* (0626DPG), and DIOG subsection 18.6.2.7.6 ("ELSUR Requirements").

4.3. This policy does not apply to notes taken by the Security Division's (SecD) Background Investigation Contract Services Unit (BICSU) special investigators (SI) in connection with background investigations. Notes generated pursuant to BICSU SI background investigation interviews are retained and destroyed by SIs in compliance with the terms of the annual basic ordering agreements (BOA) and are not FBI records nor uploaded into Sentinel.

4.4. This policy does not apply to foreign passports. They must be handled in accordance with the *Self-Reporting Requirements Policy Guide* (1037PG).

## **5. Policy Statement**

5.1. When a nontransitory, hard-copy record (needed for more than 180 days) is scanned and imported into Sentinel, the digitized version becomes the official record copy.

5.2. Nontransitory, hard-copy records must be, to the fullest extent practical, scanned and imported into Sentinel in accordance with PD 0774D, *Records Management Standards for Scanned Documents*. Documents containing text that are not available electronically must be scanned using optical character recognition (OCR) to ensure that the content is searchable in Sentinel. FBI Headquarters (FBIHQ) divisions, field offices (FO) and legal attachés (Legat) without sufficient scanning capabilities are encouraged to contact RMD Document Conversion Laboratory (DocLab) for support.

5.3. With limited exception, hard copies of nontransitory records that have been scanned, verified, and imported into Sentinel must be destroyed by the originating FBIHQ division/FO/Legat. The investigative, nontransitory, hard-copy records outlined below must be maintained in their original hard-copy formats even after being scanned and imported into Sentinel.

5.3.1. Investigative documentation that contains the handwritten text, markings, initials, or signature of a third party or non-FBI representative (e.g., a subject, a witness, a cooperator, or a partnering agency) and documents bearing the witnessed, handwritten signatures of FBI personnel.

5.3.2. Any original and notarized investigative document.

5.3.3. Any investigative document containing an original seal or an embossment.

5.3.4. Any original or certified copy of legal process involving an investigation (e.g., a subpoena, a court order, or a warrant).

5.3.5. Any original or signed copy of a national security letter (NSL) or a subpoena.

5.3.6. Any handwritten interview notes of FBI personnel. (See *Domestic Investigations and Operations Guide* [DIOG] subsection 18.5.6 for additional guidance.)

5.3.7. Any document required to be retained for financial audit purposes.

5.3.8. Any other investigative materials or documents having future evidentiary value or specifically required by applicable law or policy to be maintained in their original, hard-copy formats.

5.3.9. Any unscheduled or permanent record. Questions concerning a record's schedule (i.e., temporary, permanent, or unscheduled) should be sent via electronic mail (e-mail) to [REDACTED]

b7E

5.4. The investigative, nontransitory, hard-copy records described in subsection 5.3. of this PD must be destroyed during authorized disposition review, in accordance with FBI records retention schedules.

5.5. If the investigative, nontransitory, hard-copy records described in subsection 5.3. of this PD are created, scanned, verified, and imported by an FBIHQ division/FO/Legat other than the originating FBIHQ division/FO/Legat (e.g., an FBIHQ division/FO/Legat covering a lead), then the nonoriginating FBIHQ division/FO/Legat must send the original hard copies to the office of origin for preservation.

## 6. Rules and Responsibilities

6.1. The Office of the General Counsel (OGC) must provide legal and policy guidance to FBI personnel implementing this policy.

6.2. All FBI personnel must comply with applicable FBI policies and procedures with respect to nontransitory, hard-copy records (needed for more than 180 days).

## 7. References

- General Records Schedule (GRS) 5.2, "Transitory and Intermediary Records," Item 020
- DIOG
- Advanced Electronic Surveillance and Searches Policy Directive and Policy Guide (0626DPG)
- Digital Evidence Policy Guide (0830PG)
- Field Evidence Management Policy Guide (0780PG)
- Self-Reporting Requirements Policy Guide (1037PG)
- PD 0774D, Records Management Standards for Scanned Documents

## 8. Definitions and Acronyms

### 8.1. Definitions

8.1.1. Collected items: items and documents obtained by the FBI from a third party, including documents or items obtained via legal process (e.g., bank records or service provider records obtained via a subpoena, an NSL, a court order, or a warrant), and original volunteered documents, electronic media, or other items (e.g., receipts, original mailings with post marks, items that may contain fingerprints or other deoxyribonucleic acid [DNA] evidence, or electronic media containing documents, files, or photos). Collected items may constitute evidence and must be retained accordingly.

8.1.2. Electronic information system: an information system that provides access to computerized records and other information.

8.1.3. Federal Bureau of Investigation personnel: any individual employed by, detailed, or assigned to the FBI, including task force officers (TFO), task force members (TFM), task

UNCLASSIFIED

force participants (TFP), and members of the armed forces; an expert or a consultant to the FBI; an industrial or commercial contractor, licensee, certificate holder, or grantee of the FBI, including all subcontractors; a personal service contractor of the FBI; or any other category or person who acts for or on behalf of the FBI, as determined by the FBI Director.

8.1.4. Investigative documentation: nontransitory records generated by the government in connection with investigative and intelligence-collection activities.

8.1.5. Nontransitory record: a record needed for more than 180 days that has one or more of the following characteristics: (1) provides substantive documentation of the FBI's policies and actions, (2) contains important or valuable evidentiary information, and (3) is required to be maintained by law or regulation. A nontransitory record may have a permanent or temporary retention requirement.

8.1.6. Record: "all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government [USG] or because of the informational value of data in them; and does not include library and museum material made or acquired and preserved solely for reference or exhibition purposes; or duplicate copies of records preserved only for convenience . . . . The term 'recorded information' includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form." (Source: 44 U.S.C. Section [§] 3301)

8.1.7. Security records: security-related administrative records of FBI personnel or applicants that are not filed in investigative case file classifications.

8.1.8. Sentinel: the FBI's central recordkeeping system. It is an automated system in which nontransitory records are collected, organized, and categorized to facilitate their retrieval, use, and disposition. Sentinel provides an electronic, workflow-based environment for creating, collaborating, approving, and distributing FBI information. Sentinel provides enhanced search and analysis capabilities and facilitates information sharing with law enforcement (LE) and Intelligence Community (IC) members, including the Department of Justice (DOJ) and the Department of Homeland Security (DHS).

8.1.9. Transitory record: a temporary record that has only minimal documentary or evidentiary value and is needed for 180 calendar days or less.

8.2. Acronyms

BICSU	Background Investigation Contract Services Unit
BOA	basic ordering agreement
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DIOG	<i>Domestic Investigations and Operations Guide</i>
DNA	deoxyribonucleic acid

**UNCLASSIFIED**

DocLab	Document Conversion Laboratory
DOJ	Department of Justice
ELSUR	electronic surveillance
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FO	field office
GRS	General Records Schedule
IC	Intelligence Community
LE	law enforcement
Legat	legal attaché
NSL	national security letter
OCR	optical character recognition
OGC	Office of the General Counsel
PD	policy directive
RMD	Records Management Division
SecD	Security Division
SI	special investigator
TFM	task force member
TFO	task force officer
TFP	task force participant
U.S.C.	United States Code
USG	United States

**Approval**

**Sponsoring Executive Approval**

**Name**

**Title**

Stephen P. Rees

Assistant Director  
Records Management Division

**Final Approval**

**Name**

**Title**

David Bowdich

Associate Deputy Director